Before the
Federal Communications Commission
Washington, D.C. 20554

In the matter of	)
	)
Protecting the Privacy of Customers of	) WC Docket No. 16-106
Broadband and Other Telecommunications	)
Services	)

Reply Comments of the
Software & Information
Industry Association

Ken Wasch
President
Software and Information Industry Association
1090 Vermont Ave. NW Sixth Floor
Washington, D.C. 20004-4905
Main: +1 (202) 289-7442
Fax: 202-289-7097

July 6th, 2016

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to reply to comments on the Notice of Proposed Rulemaking, *Protecting the Privacy of Consumers of Broadband and Other Telecommunications Services* (NPRM), adopted on March 31, 2016.

SIIA appreciates the Federal Communication Commission's ("FCC" or "Commission") efforts to assess existing gaps in privacy regulations pertaining to broadband internet access service ("BIAS") providers ("broadband providers"). Indeed, by virtue of the reclassification in the 2015 Open Internet Order, broadband providers are uniquely covered by the FCC jurisdiction and there is a lack of clarity with respect to the coverage of other privacy regulations.

The Commission should reconsider its requirement of opt-in for non-sensitive data, as suggested by the FTC, and instead adopt an approach tied to the sensitivity of data.

As SIIA highlighted in our initial comments, privacy is not monolithic; it has different meanings to different individuals, across different contexts and certainly with respect to different types of data. As technologies evolve, becoming more personalized and instrumental in all facets of our lives, social norms and expectations about the flow of information and privacy also evolve along with user experiences. Therefore, policy frameworks pertaining to privacy need to remain sufficiently flexible to accommodate these evolutionary changes, where the socially beneficial uses of data made possible by data analytics are often not immediately evident to data subjects at the time of data collection.

We concur with the recommendation from the FTC staff that opt-in consent should be required for use and sharing of contents of consumer communications and sensitive data for purposes other than those for which consent implied, but that opt-out is sufficient for use and sharing of non-sensitive data.[1] As the FTC staff states in its comments referring to the NPRM proposal regarding consent for first and third-party sharing:

[1] Comments of the staff of the Bureau of Consumer Protection of the Federal Trade Commission (p. 35)

> "However, this approach does not reflect the expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful. For example, consumers may prefer to hear about new innovative products offered by their BIAS providers, but may expect protection against having their sensitive information used for this or any other purpose."[2]

SIIA strongly supports the FTC recommendation in this area, which is consistent with existing international frameworks such as the OECD Privacy Guidelines, "that the FCC consider the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to protect consumers."[3]

The Commission should reconsider its "linked or linkable" standard, in favor of the FTC's "reasonably linkable" approach, which provides a narrower, more practical framework.

As we outlined in our initial comments, SIIA is concerned that the Commission's proposed framework for defining personal information is overly broad. As we noted previously, the definition offered by the Commission, which includes, "information about or related to an individual for which there is a *possibility* of logical association with other information about the individual," [emphasis added] is so broad as to not provide for a meaningful category of information. Further, the notion of data that is only theoretically "linkable" being deemed as Personally Identifiable Information (PII) is not a widely accepted construct. The Commission suggests the possibility of advanced guidance in this area, but given the expansive definition of PII and insistence on adherence to a "linkable" standard, the result is likely to be an overly-expansive definition.

[2] Ibid (p. 22)
[3] Ibid (p. 23)

SIIA previously expressed our support for the FTC's three step test for data that "can be *reasonably* linked to a specific consumer, computer, or other device," [emphasis added] and we suggested that the Commission mirror this approach and continue to promote and provide for use of non-identifiable or de-identified data where reasonable steps have been taken to protect consumer privacy against a reasonable risk of harm. We were pleased to note the FTC staff, after reviewing the NPRM and comparing it to their current standard, made the same recommendation:

> "However, the proposal to include any data that is 'linkable' could unnecessarily limit the use of data that does not pose a risk to consumers. While almost any piece of data could be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology. FTC staff thus recommends that the definition of PII only include information that is 'reasonably' linkable to an individual."[4]

While we strongly agree with the FTC staff recommendation on this definition, we continue to disagree with the FTC objective to tie this "reasonable linkability" standard not only to individuals, but also to their devices. As we submitted to the FTC in response to proposed changes to the COPPA in 2012, expanding the definition in this way captures persistent identifiers such as cookies, static IP addresses, MAC addresses and other device and non-personal persistent identifiers that provide for a definition of personal information that often does not in any way lead to identification of a specific individual.

Persistent identifiers in use today, such as IP addresses, a processor or device serial number, or a unique device ID do not constitute "personal information," unless a provider is actually combining the information with data that identifies a specific person. Without the collection and combination with PII, these persistent identifiers are not independently useful to identify a specific individual. Therefore, collection of one or more of these types of persistent identifiers does not compromise or degrade the privacy or security of an individual, and there is no reason to believe that it will in the future.

[4] ibid (p. 10)

Contrary to the perspective offered by the FTC that internet-connected devices are becoming more personal, SIIA has found the opposite to be true. That is, in many cases these devices are becoming less personal in nature. For instance, many households already have myriad computers, tablets, smart phones, televisions, thermostats and other devices that all access the Internet. Family members migrate seamlessly between devices to access music, video, applications, social networks and a wide range of edge services. Expanded further outside of the home environment, we are also seeing the proliferation of Internet-enabled devices, appliances and vehicles that very often used by a variety of individuals, rather than tied to a single user.

The continued growth of the "Internet of Things," which is rapidly leading to an environment where devices are less personal and less linked to a particular individual, and where individuals will have access to dozens of internet-based devices in a day, some that are personal, most will likely be shared within a family or community of users.

We therefore suggest that the Commission avoid including in the definition of personal information data that is reasonably linkable to a specific device.

Multiple commenters support the FCC's view that collection of consumer information by BIAS providers raises special considerations.

In the NPRM, the Commission explained that it intended for its proposal to reach broadband internet access service (BIAS) providers, recognizing the unique financial and technical relationships BIAS providers have with their consumers. In this regard, the Commission observed that BIAS providers "have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-commerce site simply does not."[5]

[5] NPRM, p. 3

The majority of commenters correctly agreed with the Commission's approach. For example, a group of respected academics, including Nick Feamster et. al., concurred that "BIAS providers and edge providers operate extremely differently in terms of the nature of the data that they collect about customers, and the extent to which customers can control the collection of customer proprietary network data."[6] Mr. Feamster and his fellow computer scientists explore this in greater detail and conclude that "the network traffic data that edge providers collect cannot be linked to any CPNI that is collected without the user's consent; and, the data that edge providers do have about their customers is willingly provided by the customers themselves."[7]

Further exploring what network traffic data is visible to the provider, Feamster et. al. explain that while edge providers, like BIAS providers, operate networks to deliver network traffic and therefore sometimes collect information about network traffic and Internet routing to perform many of the same network management tasks that BIAS providers do, they lack the ability to tie this network data to customers.[8]

Additionally, in comments to the Commission, the FTC also highlighted findings from its 2012 Privacy Report, that, "BIAS providers have the opportunity to collect a wide range of content, as their customers interact with many different companies across the entire Internet offering diverse products and services." The FTC comments also highlighted their longstanding concerns about the ability of BIAS to use deep packet inspection of their consumers, noting, "the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a customer, without express affirmative consent or more robust protection."[9]

Comments focusing on FTC-regulated edge providers should be disregarded.

[6] Comments of Nick Feamster, et. al (p. 1)
[7] Ibid.
[8] Ibid (p. 2)
[9] Comments of the staff of the Bureau of Consumer Protection of the Federal Trade Commission (p. 20-21)

Despite this broad consensus, some commenters connected to the BIAS industry submitted comments that deviate from the Commission's proposal by raising questions about the privacy practices of so-called edge providers, which are regulated by the FTC. These comments raise issues that are outside the scope of the NPRM – and outside the scope of the Commission's statutory authority – and so they should be disregarded.

First, with respect to the scope of the proposed regulations, the FCC clearly articulates its authority over, and intent to regulate, BIAS providers covered by Section 222 of the Communications Act who have the ability to collect and share Customer Proprietary Network Information (CPNI) and directly related data. This is neither an ability that edge providers have, nor are they within the scope of the FCC's jurisdiction.

Specifically, the Commission concluded in its 2015 Open Internet Order, and reiterated in the NPRM, that Section 222 should be applied to the broadband connections that consumers use to reach the Internet, the newly-reclassified Title II service defined as BIAS, and that Section 222 "is a sector specific statute that includes detailed requirements that Congress requires be applied to the provision of telecommunications services, but not to the provision of other services by broadband provers nor to information providers at the edge of the network. Thus, this NPRM applies existing statutory authority solely to the existing class of services that Congress included within the scope of Title II, namely the delivery of telecommunications services."[10]

Second, comparisons of data collection practices by BIAS and edge providers vary. Some suggest that edge providers have greater reach for data collection, and that BIAS providers actually have less access due to encryption on the edge.[11] As noted earlier, however, the comments of Feamster and his computer science colleagues document the many ways in which BIAS providers have greater access to consumer data.

[10] See NPRM, p. 7-8, and *2015 Open Internet Order*, 30 FCC Rcd at 5820, para. 462.
[11] See comments from Comments of AT&T Services, Inc, Competitive Carriers Association and CenturyLink.

Therefore, while some commenters have tried to confuse the abilities of various edge providers and BIAS providers, there remains a distinct and inherent difference in the capabilities of BIAS and edge providers.

The proposed regulations would not negatively impact BIAS providers' ability to provide competing in offering edge services.

SIIA is concerned that some commenters incorrectly suggested that the proposed regulations would "tilt the playing field for the delivery of targeted advertisers," and "place ISPs at a substantial competitive disadvantage whenever they do offer over-the-top "edge services" in competition with non-ISP providers of those same services…"[12] The Cellular Telephone Industries Association (CTIA) went further to suggest that the proposed rules would put the "government's thumb on the scale in favor of edge providers."[13] Several other commenters make similar assertions, including the ACA, Comcast, Mobile Future and Free Software Foundation (FSF).

However, these assessments are off course. The NPRM proposes to regulate only consumer proprietary network information and personally identifying information that "a BIAS provider acquire ***in connection to its provision of BIAS***."[14] That is, if a BIAS provider wanted to launch an ad network and operate it on the same terms as an edge provider – specifically, without the use of data collected in its role as a BIAS provider – the proposed rules governing customer PII would not govern.[15] It is only if a BIAS provider wants to use information that it receives specifically in the context of its unique relationship with consumers as a BIAS provider for other purposes that additional consent obligations would apply.

The proposed regulations are overly broad.

[12] Comments of AT&T Services, Inc. (p. 55)
[13] Comments of CTIA (p. 10)
[14] Proposed Sec. 64.7000(f).
[15] To the extent that BIAS providers believe that the proposed rules are ambiguous on this point, we agree that they should be clarified.

As SIIA highlighted in our initial comments, we strongly support more flexibility than is provided in the NPRM with respect to broadband service models that rely on advertising. To that end, we noted that the proposed rule fails to recognize the benefits of innovative uses of consumer data to improve broadband service offerings for consumers, provide needed revenue for network upgrades while helping to keep costs down for consumers. And we recommended that the Commission should neither prohibit, nor discourage, information sharing-based discounts or free broadband services.